

REMARKS

Claims 1-22 are currently pending in the present application, with Claims 10-16 and 18 being preliminary amended to further clarify the claimed inventions.


Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "Version with markings to show changes made".

In the unlikely event that the transmittal letter is separated from this document and the Patent Office determines that an extension and/or other relief is required, Applicant petitions for any required relief including extensions of time and authorizes the Assistant Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 03-1952 referencing docket no. 48922.20003.00.

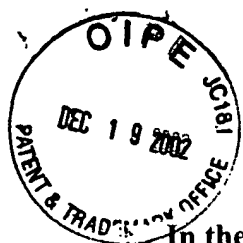
Respectfully submitted,

Dated: December 12, 2002

By:


David T. Yang
Registration No. 44,415

Morrison & Foerster LLP
555 West Fifth Street
Suite 3500
Los Angeles, California 90013-1024
Telephone: (213) 892-5587
Facsimile: (213) 892-5454



VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Claims 10-16 and 18 have been amended in the following manner:

10. (Amended) A cryptographic communication system having a pseudo-random key generator for generating cryptographic keys, said pseudo-random key generator comprising:

a pseudo-random number generator;

a timing circuit [connected] operatively coupled to said pseudo-random number generator;

a first computer readable storage [medium connected] area operatively coupled to said pseudo-random number generator, said first computer readable storage area containing a plurality of data values, each data value associated with a unique storage address within said first computer readable storage area;

[a systems re-map generator connected to said first computer readable storage medium;]

a second computer readable storage [medium connected] area operatively coupled to said first computer readable storage [medium] area, said second computer readable storage area containing a plurality of key data values, each key data value associated with a unique storage address within said second computer readable storage area,; and]

[a third computer readable storage medium connected to said timing circuit.]

wherein the pseudo-random number generator periodically generates a pseudo-random number in accordance with the timing circuit, wherein each generated pseudo-random number is used to look up a unique address in the first computer readable storage area for retrieving the data value associated with the looked up unique address, and wherein the retrieved data value is

used to look up a unique address in the second computer readable storage area for retrieving a key value data, said key value data being used to form a cryptographic key.

11. (Twice amended) The cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said first computer readable storage area for generating the data values in accordance with a predetermined algorithm [wherein said first computer readable storage medium contains a PRN re-map table].

12. (Twice amended) The cryptographic communication system according to claim [10] 11, [further comprising a systems re-map generator connected to said first computer readable storage medium,] wherein said [systems re-map generator] programmed processor selectively rearranges the data values in said first computer readable storage [medium] area.

13. (Twice amended) The cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said second computer readable storage area for generating the key data values in accordance with a predetermined algorithm

[wherein said third computer readable storage medium includes:

a key change period value; and

a crypto midnight date and time value].

14. (Twice amended) The cryptographic communication system according to claim [10] 13, wherein said [third computer readable storage medium includes a security fuse] programmed processor selectively rearranges the key data values in said second readable storage area.

15. (Amended) A method of [pseudo-randomly] generating cryptographic keys [in a cryptographic communication system having] using a pseudo-random number generator, a first computer readable storage area, and a second computer readable storage [medium] area, said method comprising the steps of:

inputting into said pseudo-random number generator [a unique systems seed value] an initial data value;

generating a pseudo-random numerical value;

generating a first data string by using said generated pseudo-random numerical value to look up a unique memory address in the first computer readable storage area and retrieving a data value associated with the unique memory address in the first compute readable storage area, said data value being one of a plurality of data values stored in the first computer readable storage area; and

generating a second data string by using said first data string to look up a unique memory address in the second computer readable storage area and retrieving a key data value associated with the unique memory address in the second compute readable storage area, said key data value being one of a plurality of key data values stored in the second computer readable storage area,

wherein the retrieved key data value is used to form a cryptographic key.

16. (Twice amended) The method according to claim 15, further comprising the steps of:

rearranging the order of the plurality of data values stored in the first computer readable storage area; and

rearranging the order of the plurality of key data values stored in the second computer readable storage area

[inputting into said computer readable storage medium a key change period value; and
inputting into said computer readable storage medium a crypto midnight date and time value.]

18. (Twice amended) The method according to claim 15, further comprising the step of initializing said computer readable storage [medium] area.